MASTER OF SCIENCE
IN
INFORMATION SYSTEMS
AND OPERATIONS

ORGANIZATIONAL STRUCTURE FOR INTER-AGENCY INFORMATION OPERATIONS

Richard K. Dougherty-Lieutenant, United States Navy
B.S., New York Maritime College, 1994
Master of Science in Information Systems and Operations-March 2001
and
Pablo F. Mir-Lieutenant, United States Navy
B.S., United States Naval Academy, 1994
Master of Science in Information Systems and Operations-March 2001
Advisors: Carl R. Jones, Information Systems Academic Group
COL Thomas H. Gerblick, United States Army

The purpose of this thesis is to stimulate a discussion toward developing an all-encompassing Inter-agency Information Operations organization. The authors define an environment and identify theories that point toward the necessity of integrating Information Operations (IO) throughout the U.S. Government (USG). The authors explore the feasibility of establishing and empowering an inter-agency organization that will monitor, evaluate and enforce all aspects of IO.

Early forms of IO and its' deployment are depicted in the historical backdrop of World War II. Concepts of renown futurists identify the importance of the Information Age and the essential process to maximize its' full potential. A correlation between the current national security strategy and the IO environment strongly suggests the need for innovation.

An overview of the current IO environment and USG organizations reveal a technological move toward inter-agency IO. Both the art and science sides of IO are incorporated into a new organization. OrgCon 7.0 is used to analyze the proposed IO organizational structure, which provides specific recommendations and defines misfits that must be addressed. The authors conclude that further work is required in modeling the organization via alternate software and a more in depth look is required in the area of national security IO. The authors provide the essential groundwork for further research.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Materials, Processes and Structures, Other (Information Operations)

KEYWORDS: Information Operations, Interagency, Interdepartmental, Organization, OrgCon, National Security

INFLUENCE NET MODELING: THE NARCOTICS NETWORK IN COLOMBIA

Mark W. Garrett-Major, United States Army
B.L.A., Texas Tech University, 1988
Master of Science in Information Systems and Operations-March 2001
and
Joshua C. Himes-Lieutenant, United States Navy
B.A., University of Pennsylvania, 1993
Master of Science in Systems Technology-June 2001
Advisors: LT Raymond R. Buettner, Jr., USN, Information Warfare Academic Group
Jeanne K. Giraldo, Department of National Security Affairs

The purpose of this thesis is to conduct the research necessary to develop a situational influence assessment model to identify critical indicators that will assist the USSOUTHCOM in identifying potential key centers of gravity in the fight against illicit drug production and narcotrafficking in Colombia. Efforts to combat the narcotics network directly support the USSOUTHCOM mission and are integral to U.S. National Security. Unlike the traditional military threats of the Cold War and previous decades, to include *Operation Desert Storm*, this problem set is far more complex and complicated with roots and foundations that date back to the development of Colombia as a nation-state. It is the strategic dilemma that is posed by this asymmetric threat that reflects the type of problems that will be encountered by the military of the 21st century. Unlike the traditional land/sea/air combined warfare that the U.S. dominates globally, the threats of the 21st century will look much like Colombia – small, packetized, networked organizations with the ability to operate and inflict casualties below the threshold of our traditional military mechanisms. Improved decision support systems to model this type of problem are needed. This thesis suggests a number of modifications to an existing model, SIAM, in order to enhance its usefulness both for decision makers and intelligence collectors.

DoD KEY TECHNOLOGY AREA: Other (Information Operations, Intelligence Information Management)

KEYWORDS: Information Operations, Intelligence, Decision Support Systems, Influence Net Modeling, Colombia

A DISCRETIONARY-MANDATORY MODEL AS APPLIED TO NETWORK CENTRIC WARFARE AND INFORMATION OPERATIONS

Daniel R. Hestad-Lieutenant, United States Navy
B.S., University of Wisconsin, 1994
Master of Science in Information Systems and Operations-March 2001
Advisors: J. Bret Michael, Department of Computer Science
Audun Josang, Queensland University of Technology

The concepts of DoD information operations and network centric warfare are still in their infancy. In order to develop these concepts, the right conceptual models need to be developed from which to design and implement these concepts. Information operations and network centric warfare are fundamentally based on trust decisions. However, the key to developing these concepts is to develop for DoD is to develop the organizational framework from which trust, inside and outside, of an organization may be achieved and used to its advantage. In this thesis, an organizational model is submitted for review to be applied to DoD information systems and operational organizations.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software

KEYWORDS: Trust Models, Trust Management, Computer Security, Information Operations

MODELING INFLUENCES ON NUCLEAR WEAPONS DECISION MAKING BY PAKISTAN USING THE SITUATIONAL INFLUENCE ASSESSMENT MODEL PROGRAM

Bradley J. Kidwell-Lieutenant Commander, United States Navy
B.S., San Jose State University, 1987
and
Jeremy P. Jurkoic-Lieutenant, United States Navy
B.S., United States Naval Academy, 1995
Master of Science in Information Systems and Operations-March 2001
Advisors: LT Raymond R. Buettner, Jr., USN, Information Warfare Academic Group
James J. Wirtz, Department of National Security Affairs

Since Pakistan's inception in 1947, when the British carved it out of the western region of India, Pakistan and India have fought three wars and even now coexist in a permanent state of tension. Since 1998, both nations have declared their nuclear status, creating a risk of nuclear war in any future conflict. Low-level skirmishes between Indian and Pakistani forces along the Line-of-Control (LOC) in the disputed state of Kashmir are a regular occurrence, providing the most likely scenario for full-scale warfare to erupt between India and Pakistan. Further, the disparity of conventional forces between India and Pakistan (India enjoys a 2:1 conventional force superiority over Pakistan) has spurred Pakistan's nuclear program, and provides significant impetus for Pakistan to resort to first use of nuclear weapons. Pakistan views their nuclear weapons as both a deterrent and a force multiplier.

Utilizing a computer program known as Situational Influence Assessment Module (SIAM), an influence net model is constructed to ascertain the likelihood of Pakistan using nuclear weapons against India. The model is used to examine U.S. Central Command's (CENTCOM) Theater Engagement Plan (TEP) goals and whether or not the TEP effectively targets the key influences identified in the model.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Modeling and Simulation

KEYWORDS: Pakistan, Nuclear Weapons, Modeling and Simulation, SIAM, Information Warfare, Perception Management

THE EMPLOYMENT OF A WEB SITE AND WEB-ENABLING TECHNOLOGY IN SUPPORT OF U.S. MILITARY INFORMATION OPERATIONS

James T. Mayer-Major, United States Army
B.S., Centre College of Kentucky, 1989
Master of Science in Information Systems and Operations-March 2001
Advisors: J. Bret Michael, Department of Computer Science
LT Raymond R. Buettner, Jr., USN, Information Warfare Academic Group

As a global-based system of information systems, the World Wide Web has the potential to support U.S. Military Information Operations. Presently, there is a lack of established U.S. Military Doctrine or Planning Guidance on how to incorporate the use of a website in support of Information Operations (IO). This thesis proposes suitable uses of a web site within the IO arena as defined by Joint Military Doctrine. Specifically, it is proposed that a web site can support all of the following type of activities: public information, civil affairs, psychological operations, deception and intelligence collection. In addition, the U.S. commercial marketing sector is advantageously employing recent advances in Information Technology and software which have yielded web-enabling features such as interactivity, personalization, customization, and dynamic information publishing, to name a few. The U.S. military can learn a great deal from this. This thesis describes some recent web-enabling technology and then provides a first approximation at mapping web-enabling features to IO capabilities. One product of this thesis is a first approximation of a planning checklist to be used by IO practitioners and web-site developers when considering the use of a web-based IO. Although technology will continue to change, this planning checklist provides a template for integrating web-enabling features within IO.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Information Operations, Website, Web-enabling Technology, Personalization, Dynamic Information Publishing

TRUST AND ITS RAMIFICATIONS FOR THE DOD PUBLIC KEY INFRASTRUCTURE

Carl M. Pedersen-Lieutenant, United States Navy
B.S., Oregon State University, 1995
Master of Science in Information Systems and Operations-March 2001
Advisor: J. Bret Michael, Department of Computer Science
Audun Josang, Queensland University of Technology

Researchers have used a wide variety of trust definitions, leading to a plethora of meanings of the concept. But what does the word 'trust' mean? While most scholars provide their own definition of trust, they are dissatisfied regarding their own lack of consensus about what trust is. Trust is a cognitive function and modeling trust is an attempt to emulate the way a human assesses trust. Models of trust have been developed in an attempt to automate the logic, variables, and thought processes that a human performs when making a trust-decision. This thesis evaluates the various forms of trust and trust models. The results from our research found no such model that incorporates both mandatory and discretionary trust. A new hybrid model will be introduced, the "D-M Model." The motivation for using the model in the context of trust stems primarily from the appropriate use of discretionary and mandatory trust policies in organizations to ensure precision, consistency, and added assurance in trust. The real value of the D-M model, is that it addresses the need to model both of these types of policies explicitly and concurrently. This thesis concludes with the assessment of two practical applications of the D-M trust model as it is applied to DoD's Joint Task Forces.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Trust Models, Trust Management, Public Key Infrastructure (PKI), Computer Security